Homework 18 Solutions

1. **The goal of this problem is to find** $5/17 \pmod{31}$**. Note that 31 is prime, and thus we know that a solution exists.**

   (a) **Use the Euclidean Algorithm to find integers** x **and** y **such that** $17x + 31y = 1$**.**
   The Euclidean algorithm gives

   $$\begin{aligned} 31 &= 17 + 14 \\ 17 &= 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 2 + 1. \end{aligned}$$

   Running it backwards, we have

   $$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (14 - 4 \cdot 3) = -14 + 5 \cdot 3 \\ 1 &= -14 + 5(17 - 14) = 5 \cdot 17 - 6 \cdot 14 \\ 1 &= 5 \cdot 17 - 6(31 - 17) = -6 \cdot 31 + 11 \cdot 17. \end{aligned}$$

   So we can take $\boxed{x = 11 \text{ and } y = -6}$.

   (b) **Using part (a), what is** $1/17 \pmod{31}$**?**
   Part (a) tells us that $11 \cdot 17 = 1 + 6 \cdot 31 \equiv 1 \pmod{31}$. This is equivalent, by definition, to the fact that $1/17 \equiv \boxed{11} \pmod{31}$.

   (c) **Now multiply your answer to part (b) by 5 to find** $5/17 \pmod{31}$**.**
   We have

   $$5/17 \equiv 5 \cdot 1/17 \equiv 5 \cdot 11 \equiv 55 \equiv \boxed{24} \pmod{31}.$$

2. **Do the following divisions.**

   (a) $7/10 \pmod{40}$.
   It's clear that 10 and 40 are not relatively prime (their gcd is 10), and thus division by 10 isn't defined in arithmetic mod 40. So the answer is $\boxed{\text{does not exist}}$.

   (b) $9/23 \pmod{40}$.
   The Euclidean algorithm gives

   $$\begin{aligned} 40 &= 23 + 17 \\ 23 &= 17 + 6 \\ 17 &= 2 \cdot 6 + 5 \\ 6 &= 5 + 1. \end{aligned}$$

   This shows that 23 and 40 are relatively prime, and thus this division is well-defined. Running it backwards, we have

   $$\begin{aligned} 1 &= 6 - 5 \\ 1 &= 6 - (17 - 2 \cdot 6) = -17 + 3 \cdot 6 \\ 1 &= -17 + 3(23 - 17) = 3 \cdot 23 - 4 \cdot 17 \\ 1 &= 3 \cdot 23 - 4(40 - 23) = -4 \cdot 40 + 7 \cdot 23. \end{aligned}$$

   This shows that $1/23 \equiv 7 \pmod{40}$. Finally, we have

   $$9/23 \equiv 9 \cdot 1/23 \equiv 9 \cdot 7 \equiv 63 \equiv \boxed{23} \pmod{40}.$$

(c) $10/2 \pmod{31}$.

It's clear that 2 and 31 are relatively prime (since 31 is odd), and thus this division is well-defined. It's also clear that $2 \cdot 5 \equiv 10 \pmod{31}$, which means that $10/2 \equiv \boxed{5} \pmod{31}$.

(d) $5/16 \pmod{17}$.

Again, we see that 16 and 17 are relatively prime, so this division is well-defined. Note that $16 \equiv -1 \pmod{17}$. Using this, we have

$$5/16 \equiv 5/-1 \equiv -5 \equiv \boxed{12} \pmod{17}.$$

(e) $10/2 \pmod{20}$.

Obviously, 2 and 20 are not relatively prime, since 2 divides 20. Thus division by 2 is not defined in arithmetic mod 20, and the answer is $\boxed{\text{does not exist}}$. This is correct even though this division is well-defined in ordinary arithmetic. In particular, one might be tempted to say the answer is 5 because $2 \cdot 5 \equiv 10 \pmod{20}$, but $2 \cdot 15 \equiv 10 \pmod{20}$ also, and so we have the problem of non-uniqueness as discussed in lecture.

(f) $1/9 \pmod{44}$.

The Euclidean algorithm gives

$$\begin{aligned} 44 &= 4 \cdot 9 + 8 \\ 9 &= 8 + 1. \end{aligned}$$

This shows that 44 and 9 are relatively prime, and thus this division is well-defined. Running it backwards, we have

$$\begin{aligned} 1 &= 9 - 8 \\ 1 &= 9 - (44 - 4 \cdot 9) = -44 + 5 \cdot 9. \end{aligned}$$

This shows that $1/9 \equiv \boxed{5} \pmod{44}$.